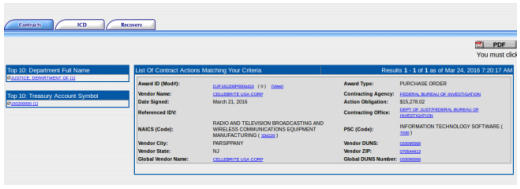
iPhone chiffré : une boîte israélienne à la rescousse du FBI ?



iPhone chiffré : une boîte israélienne à la rescousse du FBI ?

Lundi 21 mars, le FBI a pris tout le monde de court en annonçant avoir trouvé une solution pour accéder aux données stockées sur l'iPhone chiffré de l'un des co-auteurs de la tuerie de San Bernardino, Syed Farook.
Après avoir aboyé partout que seul Apple pouvait débloquer la situation, l'administration américaine a en effet affirmé avoir reçu l'aide d'un mystérieux « tiers », annulant ainsi une confrontation prévue le lendemain même devant une cour de Californie.
En attendant le compte-rendu de cette méthode, que la justice attend d'ici le 5 avril, la presse spécialisée spécule sur l'identité de l'auxiliaire-mystère. Et avance un nom : Cellebrite.

Maître du « digital forensics »

Pour Yedioth Ahronoth (en hébreu), qui cite des sources anonymes, cela ne fait même aucun doute : c'est bien cette boîte israélienne qui a aidé le FBI.
Vidéo promotionnelle d'une solution de Cellebrite, permettant de débloquer un iPhone
Si les deux intéressés se sont refusés à tout commentaire, les spécialistes de l'informatique et du renseignement estiment l'information probable.
Il faut dire que cette firme, établie depuis 1999, est l'une des rares à maîtriser l'art du « digital forensic » dans la téléphonie mobile et le GPS.
Soit la dissection des appareils numériques, dans le cadre notamment d'enquêtes.
Le chercheur David Billard, sollicité en tant qu'expert dans des affaires de ce genre et rattaché à la cour d'appel de Chambéry, détaille :
« Le digital forensic consiste à récupérer les preuves, ou éléments de preuve, dans des appareils numériques. […]
Par exemple, extraire des vidéos d'un ordinateur dans le cadre d'une enquête sur un viol, retrouver des SMS effacés d'un téléphone portable dans le but de confirmer, ou infirmer, une complicité, etc… »

Analyse des appareils brûlés, écrasés, chiffrés…

*Or en la matière, l'inventaire de Cellebrite est fourni. **Promet de venir à bout** de matériel protégé par un mot de passe, « écrasé, cassé, brûlé ou endommagé par l'eau ». Et, plus intéressant en l'espèce :*
« d'analyser des formats d'application de données et des méthodes de chiffrement complexe et inconnu. »
*Le FBI semble d'ailleurs parfaitement conscient de ces compétences puisque l'agence a noué de nombreux contrats avec Cellebrite, relève le journaliste américain **John Paczkowski**, qui est allé fouiller dans les bases de données publiques de l'administration. A chaque fois, il est question d'acquisition de matériel de télécommunication, sans fil, relatif à l'informatique, par le ministère de la justice américain (le DOJ).*

*L'accord conclu entre Cellebrite et le FBI, le 21 mars 2016 – **DPSD / gouvernement américaine***
*En tout, 2 millions de dollars auraient ainsi été dépensés depuis 2012, **écrit Motherboard**. Qui relève un autre détail intéressant : **le 21 mars 2016**, soit le jour de l'annonce-surprise du FBI, un accord de 15 000 dollars a justement été signé avec Cellebrite.*

Cellebrite déjà sollicité… sans succès

Avant même que le journal israélien pointe explicitement vers Cellebrite, son nom revenait de toute façon déjà dans les articles sur la saga opposant le FBI à Apple.
*L'expert des appareils d'Apple Jonathan Zdziarski **prévenait déjà en septembre 2014** : malgré les précautions louables de la marque, les derniers systèmes d'exploitation de l'iPhone ne sont pas totalement inviolables. Et Cellebrite faisait selon lui parti des rares entreprises capables de fournir des solutions commerciales pour accéder aux données du téléphone.*
*Il ne pouvait être plus proche de la vérité : dans une déclaration remise à la cour appelée à trancher le contentieux entre Apple et le FBI, un ingénieur de l'agence explique avoir déjà eu recours aux services de cette entreprise ! Sans succès… jusque là, **rapporte le New York Times** ce jeudi.*

Nombreux faits d'armes

*Par le passé aussi, Cellebrite s'est démarqué par quelques faits d'armes évocateurs. Début 2016, c'était pour **avoir aidé la police néerlandaise** à lire les messages chiffrés et supprimés d'un Blackberry.*
*Huit ans auparavant, l'association américaine en défense des libertés civiles, l'ACLU, **se lançait dans une procédure** contre la police du Michigan, accusée d'utiliser illégalement les outils de Cellebrite pour fouiller dans les téléphones des suspects.*
*Au nom du Freedom of Information Act (le FOIA), l'organisation **a demandé la publication** de compte-rendus sur l'utilisation de cette solution technique. La police a rétorqué que cette publication lui coûtait des centaines de milliers de dollars et, à notre connaissance, l'ACLU n'a toujours rien reçu… [Lire la suite]*

Réagissez à cet article

Source : *iPhone chiffré : une boîte israélienne à la rescousse du FBI ? – Rue89 – L'Obs*

L'iPhone du tueur débloqué par le FBI. Fin des poursuites contre Apple

L'iPhone du tueur débloqué par le FBI. Fin des poursuites contre Apple

---

Les autorités américaines affirment avoir « accédé avec succès aux données contenues dans l'iPhone de Syed Farook » et ont demandé à la justice d'annuler l'injonction obligeant la firme à la pomme à assister les enquêteurs.

Ce déblocage a été rendu possible par *« l'assistance récente d'un tiers »* (ndlr Cellebrite), selon un communiqué de la procureure fédérale du centre de la Californie, Eileen Decker. Elle indique en conséquence avoir demandé à la justice d'annuler l'injonction obligeant Apple à aider les enquêteurs. La firme refusait de se plier aux demandes judiciaires, soutenant qu'aider à décrypter le téléphone de Syed Farook créerait un précédent, sur lequel les autorités risquaient de s'appuyer à l'avenir pour réclamer l'accès aux données personnelles de nombreux citoyens pour diverses raisons.

« Viabilité »

Lundi 21 mars, les autorités fédérales avaient annoncé être sur la piste d'une méthode qui pourrait leur permettre d'accéder aux données du téléphone. Une audience clé, qui devait avoir lieu mardi au tribunal de Riverside en Californie, avait été annulée, après le dépôt d'une motion demandant un délai pour tester *« la viabilité »* de cette solution alternative.

Le gouvernement expliquait avoir *« poursuivi ses efforts pour accéder à l'iPhone »* pendant la procédure judiciaire et annonçait que des *« tierces parties »* lui avaient présenté une manière de décrypter son contenu sans la coopération d'Apple. La police fédérale demandait un peu de temps pour s'assurer que la méthode ne *« détruit pas les données du téléphone ».*

Une semaine plus tard, il semble donc que la méthode fonctionne. Washington affirme à la cour fédérale avoir *« accédé avec succès aux données contenues dans l'iPhone de Syed Farook »* et *« ne plus avoir besoin de l'assistance d'Apple »*… [Lire la suite]

Réagissez à cet article

Source : *San Bernardino : Washington a débloqué l'iPhone du*

tueur et renonce à poursuivre Apple

Alerte : 6 millions d’iPhones victimes d’un Trojan qui exploite un bogue du DRM ?

Alerte : 6 millions d’iPhones victimes d’un Trojan qui exploite un bogue du DRM ?

D’après Palo Alto Networks, un nouveau malware baptisé AceDeceiver, a déjà infecté près de 6 millions d’appareils iOS non jailbreakés appartenant à des utilisateurs Chinois.

Comme ont pu le constater les chercheurs, ce trojan infecte les appareils mobiles via des ordinateurs Windows et exploite des erreurs commises par Apple dans le système de gestion des droits numériques (DRM). A l’heure actuelle, AceDeceiver circule uniquement sur le territoire chinois ; d’après Palo Alto, il s’agirait du premier malware capable d’infecter les gadgets d’Apple qui utilisent le système imparfait DRM FairPlay. Et il n’est pas nécessaire que l’appareil soit débridé pour garantir l’infection.

« D’abord, il y a eu XcodeGhost, puis ZergHelper, et maintenant AceDeceiver » a rappellé Ryan Olson, directeur des études sur les virus chez Palo Alto, alors qu’il commentait la dernière découverte aux journalistes de Threatpost. « Ils contribuent tous à l’érosion continue de la protection du magasin d’applications d’Apple ». D’après l’expert, AceDeceiver permet d’obtenir un accès « homme au milieu » à l’appareil iOS et de forcer l’utilisateur à communiquer son identifiant Apple aux attaquants.

Ce nouveau malware iOS se distingue de ses prédécesseurs par le fait qu’il n’utilise pas de certificats légitimes Apple pour s’introduire dans un appareil non débridé. Il opte pour la technique FairPlay Man-In-The-Middle, utilisée déjà depuis deux ans pour diffuser des applications pirates. D’après les conclusions de Palo Alto, le trojan AceDeceiver est le premier cas où ce genre de modification est utilisé pour installer des malwares sous iOS à l’insu de l’utilisateur.

L’analyse a démontré que les auteurs d’AceDeceiver ont préparé cette campagne malveillante pendant de nombreux mois. Au deuxième semestre de l’année dernière, ils ont réussi à introduire dans l’App Store trois versions différentes de l’application AceDeceiver avec une fonction d’économiseur d’écran. Cette opération s’imposait afin d’obtenir les codes d’autorisation d’Apple sollicités via iTunes. Par la suite, les individus malintentionnés ont exploité ces codes avec l’application Windows Aisi Helper spécialement développée à cette fin pour procéder à l’installation des malwares sur les appareils mobiles à l’insu de l’utilisateur.

Aisi Helper est vendu uniquement en Chine et se présente comme un outil pour iOS qui permet de créer des copies de sauvegarde, de restaurer le système, de débrider les appareils, d’administrer l’appareil et de le purger. Toutefois, dans ce cas l’existance d’un client de ce genre sur le poste de travail Windows simplifie également la tâche de l’attaquant car le malware peut être installé sur les appareils iOS lorsque ceux-ci sont connectés à l’ordinateur. AceDeceive réalise l’installation en substituant la poigné de main FairFlay par son propre serveur d’autorisation. Il s’agit d’une attaque FairPlay Man-In-The-Middle, appliquée pour la première fois en 2014.

AceDeceiver a été porté à l’attention d’Apple le mois dernier et la société a déjà retiré les trois faux économiseurs d’écran de son magasin d’applications. Palo Alto indique toutefois que l’attaque est toujours possible. « Tant que les attaquants disposent du code d’autorisation, ils ne doivent pas obligatoirement accéder à l’App Store pour diffuser ses applications » expliquent les chercheurs dans leur blog. Ryan Olson, de son côté, a confirmé aux journalistes que de telles utilisationsdétournées étaient possibles car les résultats de l’analyse réalisée par le mécanisme DRM d’Apple sont valides en dehors de l’écosystème iTunes.

Une fois installé sur un appareil iOS, AceDeceiver peut fonctionner comme un magasin d’applications alternatifs. Il fonctionne sous le contrôle des individus malintentionnés et offre un large choix de jeux et d’utilitaires. L’utilisateur est également invité à saisir son identifiant Apple et son mot de passe pour pouvoir accéder à toutes les fonctions de l’application pirate gratuite.

Ryan Olso explique qu’il est difficile d’éliminer les problèmes provoqués par AceDeceiver. Dans le cas de ZergHelper cité ci-dessus, Apple avait simplement supprimé le malware de son magasin. Le nouveau trojan se distingue par le fait qu’il compte sur un client Windows et utilise un code d’autorisation obtenu antérieurement, ainsi que des lacunes dans le projet FairPlay DRM.

Au moment de la publication de ce billet, Apple n’avait pas encore réagi aux questions de Threatpost…. [Lire la suite]

Réagissez à cet article

Source : *Un Trojan Exploite Un Bogue Du DRM Pour Charger Des Malwares Dans IOS – Securelist*

Le FBI pense pouvoir déchiffrer l’iPhone d’un terroriste sans l’aide d’Apple

Le FBI pense pouvoir déchiffrer l’iPhone d’un terroriste sans l’aide d’Apple

Alors qu'Apple refuse depuis des semaines d'aider le FBI à décrypter l'iPhone de l'un des auteurs de la tuerie de San Bernardino, le FBI vient d'annoncer qu'il tenait peut-être la solution.

La fin d'un bras de fer?

Le gouvernement américain pourrait ne plus avoir besoin des services d'Apple pour récupérer les données de l'iPhone de l'un des terroristes de l'attaque de San Bernardino survenue le 2 décembre 2015. Il a annoncé ce lundi être sur la piste d'une solution alternative. Si elle s'avère efficace, cela mettrait fin à la bataille juridique engagée depuis des semaines avec la marque à la pomme.
Une audience clé qui devait avoir lieu mardi a finalement été levée sur la demande des autorités fédérales. Les enquêteurs vont ainsi pouvoir tester « la viabilité » de leur « méthode ». Ils se sont engagés à remettre à la juge Sheri Pym d'ici le 5 avril, un rapport d'évaluation.

Les autorités optimistes

Dans un communiqué, le ministre de la justice a indiqué qu'il avait poursuivi ses efforts pour accéder à l'iPhone sans l'aide d'Apple depuis de le début de la procédure engagée contre la firme de Cupertino. Les recherches ont abouti dimanche avec la « présentation de la part de tierces parties d'une méthode possible pour débloquer le téléphone », indique le communiqué. Le gouvernement veut s'assurer que sa solution « ne détruit pas les données du téléphone », mais reste « raisonnablement optimiste ».
Les enquêteurs et les familles des victimes réclament de pouvoir accéder aux données du téléphone, potentiellement cruciales pour déterminer comment a été organisé l'attentat et si les deux terroristes ont bénéficié d'aide extérieure.

Apple de son côté campe sur ses positions

Permettre d'accéder aux données du téléphone de Syed Farook créerait un dangereux précédent qui pourrait justifier que les autorités demandent à l'avenir l'accès aux données personnelles de nombreux citoyens pour diverses raisons.
A l'occasion de la keynote d'Apple qui s'est tenue lundi, Tim Cook a justifié la position de la marque. « Nous devons décider en tant que nation quel pouvoir devrait avoir le gouvernement sur nos données et notre vie privée », a-t-il déclaré. « Nous pensons fermement que nous avons l'obligation d'aider à la protection de vos données et votre vie privée », a-t-il ajouté.
Pour rappel, le 2 décembre 2015, Syed Farook et sa femme Tashfeen Malik ont ouvert le feu dans un centre social à San Bernardino, dans l'Etat de Californie. 14 personnes ont été tuées dans la fusillade … [Lire la suite]

Réagissez à cet article

Source : *Le FBI pense pouvoir déchiffrer l'iPhone d'un terroriste sans l'aide d'Apple – L'Express*

Un nouveau logiciel malveillant cible les iPhone | Le Net Expert Informatique

Décidément, les terminaux à la pomme intéressent de plus en plus les pirates. Après la découverte le 4 février par les experts du cabinet de sécurité informatique Trend Micro du premier logiciel espion baptisé « XAgent » exploitant des failles sur les téléphones Apple non débridés (dits « non jailbreakés »), c'est au tour de l'unité de recherche 42 de l'entreprise de sécurité informatique Palo Alto Networks de publier dimanche 4 octobre une alerte sur un nouveau logiciel malveillant (malware) affectant les iPhones du commerce.

Baptisé « YiSpecter », il attaque sans distinction les iPhone du commerce vendus avec le système d'exploitation officiel iOS d'Apple et ceux qui ont été débridés. Apple, qui a reconnu l'existence de ce malware, a indiqué lundi 5 octobre que les utilisateurs d'iOS 8.4 et d'iOS 9 étaient désormais protégés. La particularité de ce programme – qui serait actif depuis plus de 10 mois à Taïwan et en Chine continentale d'où il proviendrait – est d'utiliser des failles que l'on pensait impossible à exploiter, et de se propager de façon inédite, selon Palo Alto Networks.

Un fonctionnement et une propagation inédits

Détournant certaines interfaces de programmation propres au système d'exploitation iOS, cette nouvelle forme de logiciel malveillant ne laisse rien présager de bon pour l'avenir des terminaux mobiles à la pomme selon la firme de sécurité à l'origine de la découverte : « C'est le premier malware que nous avons vu en circulation qui abuse les API [interfaces de programmation] privées dans le système iOS pour mettre en œuvre des fonctionnalités malveillantes. »

En se propageant seul soit grâce à « Lingdun », un ver informatique sous Windows (qui se charge d'envoyer des liens malicieux de téléchargement d'YiSpecter à tous ses contacts), soit par le piratage des connexions WiFi des boîtiers des fournisseurs d'accès à Internet, cette nouvelle variante de malware inquiète la société californienne. Ses quatre composants, tous authentifiés par des certificats d'entreprises réels émanant de sociétés comme Verisign ou Symantec, s'installent de façon furtive sur les iPhone, en masquant ses programmes, mais aussi en dupliquant les noms et les logos des icônes système (Game Center, Météo, Notes, PassBook, Téléphone, etc.), piégeant même les utilisateurs les plus avertis.

Une fois installé, YiSpecter peut télécharger, installer et lancer des applications de l'App Store, mais aussi les modifier, par l'affichage de publicités en plein écran par exemple. Il permet également de collecter les données des utilisateurs, notamment celles utilisées dans le navigateur Internet Safari. S'il est découvert, sa suppression par méthode classique ne fonctionnera pas car il se réinstalle automatiquement après un redémarrage système. Enfin, peu d'espoir du côté des antivirus, qui ne détectent toujours pas sa présence sur les terminaux infectés.

Des malwares aux origines peu claires

Certains indices repérés par Palo Alto Networks font converger les soupçons vers « YingMob », une entreprise chinoise de publicité mobile ayant pignon sur rue, qui aurait programmé et diffusé ce malware à des fins publicitaires, n'hésitant pas à en faire sa promotion au grand jour. Mais la complexité et les méthodes de propagation de YiSpecter cachent peut-être des visées plus opaques.

Déjà le mois dernier, 344 applications iOS officielles présentes dans l'App Store, la boutique d'applications d'Apple, avaient été retirées en urgence car infectées par le malware « XcodeGhost », découvert le mercredi 16 septembre par les équipes sécurité du groupe chinois Alibaba. L'origine de ce malware est encore incertaine, mais les méthodes utilisées sont très similaires aux techniques de programmation qu'emploie la CIA – selon des documents publiés en mars par The Intercept.

Tout début septembre, c'était le logiciel malveillant « KeyRaider » également découvert par la société Palo Alto Networks, qui faisait parler de lui : selon la société de sécurité, plus de 225 000 comptes et identifiants Apple auraient été dérobés, uniquement sur des iPhone et iPad débridés.

La société de sécurité américaine est également à l'origine de la chute d'un mythe : c'est elle qui annonçait il y a moins d'un an, en novembre 2014, la découverte, toujours en Chine, de « Wirelurker », le tout premier malware pour iPhone touchant des téléphones non débridés. Depuis, il ne se passe pas un mois sans qu'une nouvelle alerte concernant les terminaux mobiles d'Apple ne soit lancée.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Source :
http://www.lemonde.fr/pixels/article/2015/10/07/un-nouveau-logiciel-malveillant-cible-les-iphone_4784509_4408996.html

Liste des applications iPhone et iPad infectées par le logiciel malveillant XcodeGhost | Le Net Expert Informatique

	Liste des applications iPhone et iPad infectées par le #logiciel malveillant XcodeGhost

Des experts en sécurité ont récemment découvert sur un certain nombre d'applications dans l'App Store d'Apple un maliciel iOS appelé XcodeGhost. Les créateurs de XcodeGhost ont été en mesure d'intégrer un code malveillant dans ces applications à l'insu de leurs développeurs. Parmi les applications touchées, on retrouve les populaires WeChat et CamCard. Nous pouvons donc estimer que le nombre de victimes potentielles du logiciel malveillant XcodeGhost s'élèverait à de centaines de millions d'utilisateurs.

Voici une liste non exhaustive des applications détectées en tant que malveillantes :

CamCard Business
Action: Update to latest version
Current Status: Patched
Last version checked: 1.8.2

CamScanner Free| PDF Document Scanner and OCR
Action: Update to latest version
Current Status: Patched
Last version checked: 3.8.2

CamScanner +| PDF Document Scanner and OCR
Action: Update to latest version
Current Status: Patched
Last version checked: 3.8.2

Cam Scanner Pro
Action: Update to latest version
Current Status: Patched
Last version checked: 3.8.2

WeChat
Action: Update to latest version
Current Status: Patched
Last version checked: 6.2.6

WinZip – The leading zip unzip and cloud file management tool
Action: Update to the latest version
Current Status: Patched
Last version checked: 4.3

网易云音乐-好口碑,电台FM歌曲下载必备
Action: Update to latest version
Current Status: Patched
Last version checked: 2.9.0

OPlayerHD Lite
Action: Update to latest version
Current status: Patched
Last version checked: 2.1.03

网易公开课 — 教育视频平台，名校名师名课，TED演讲、优质纪录片
Action: Update to latest version
Current Status: Patched
Last version checked: 4.2.9

LifeSmart
Action: Uninstall immediately
Current status: Still malicious
Last version checked: 1.0.45

10000+ Wallpapers for iOS 8, iOS 7, iPhone, iPod and iPad
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 3.6

喜马拉雅FM (Podcasts) 儿童故事评书段子财经相声radio
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 4.3.8

开眼 — 精选视频推介，每天大开眼界
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 1.8.0

愤怒的小鸟2-李易峰至尊手游
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 2.1.1

爱推
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 1.1.5

电话号码归属地助手
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 3.6.5

自由之战-真·5V5(第一MOBA手游)
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 1.1.0

中国联通手机营业厅(官方版)
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 3.2

股市热点
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 2.40.01

Plus d'infos sur : https://blog.lookout.com/blog/2015/09/21/xcodeghost-apps

---

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : https://blog.
lookout.com/fr/2015/09/23/xc
odeghost-apps/

Des hackers dupent Apple et infectent des millions d’iPhone | Le Net Expert Informatique

Des hackers dupent Apple et infectent des millions d’iPhone

Pour la première fois, des pirates ont réussi à diffuser des applications malveillantes sur le magasin AppStore, en trafiquant le langage de codage utilisé par les développeurs.

Après ses ordinateurs Mac, c'est au tour des iPhone et iPad d'Apple de se frotter aux virus. Le groupe à la pomme croquée a confirmé à Reuters que son magasin d'applications AppStore a été victime de sa toute première faille de sécurité majeure. Jusqu'à présent, l'AppStore était réputé comme ultra-sûr puisqu'Apple inspecte minutieusement chaque appli avant de la proposer aux téléchargements (à l'inverse du Play Store de Google), afin d'éviter les logiciels malveillants mais aussi imposer sa chape de plomb sur le sexe.

Sauf que des pirates malins ont trouvé une parade pour échapper à la vigilance de la pomme. Les hackers sont remontés jusqu'à la source de toutes les applis, le langage de codage Xcode, pour diffuser auprès des développeurs naïfs une version compromises (intitulée XcodeGhost). Toutes les applis créées avec cet outil pouvant dès lors de se transformer en logiciel malveillant. Un porte-parole d'Apple souligne auprès de Reuters :

Nous travaillons avec les développeurs afin de garantir qu'ils utilisent la version authentique de Xcode pour redévelopper leurs apps ».

La version compromise de Xcode a été identifiée comme hébergée sur un serveur chinois. Les développeurs ont préféré celle-ci puisqu'elle s'avérait beaucoup plus rapide à télécharger que le logiciel officiel hébergé sur le serveur d'Apple.

Des centaines de millions d'iPhone exposés

Selon la firme de sécurité Palo Alto Networks Inc, 39 applications malicieuses ont été découvertes et certaines sont particulièrement populaires, dont :

– l'incontournable appli de discussion instantanée WeChat,
– le très utilisé enregistreur de cartes de visites CamCard,
– Didi Chuxing, le concurrent chinois d'Uber,
– l'unique appli pour acheter des billets de train en Chine Railway 12306.

Au total, plusieurs centaines de millions d'utilisateurs pourraient avoir été victimes d'un vol de données tels que des mots de passe, estime l'entreprise, même si aucun cas n'a pour l'heure été constaté.

La firme de sécurité chinoise Qihoo360 affirme elle avoir détecté pas moins de 344 applis compromises. Plusieurs ont été retirées de l'AppStore par Apple, mais le groupe refuse de donner le nombre exact d'applications concernées. Un porte-parole affirme à « l'Obs » : *Nous prenons la sécurité très au sérieux et iOS [le système de l'iPhone et l'iPad, NDLR] est conçu pour être fiable et sécurisé. Pour protéger nos clients, nous avons supprimés les applications de l'AppStore que nous savons créées avec cet outil contrefait. »*

Sur son blog, WeChat affirme que seule la version de son appli antérieure au 10 septembre était affectée par la faille de sécurité. Une nouvelle version a depuis été diffusée pour remédier au problème.

Les iPhone, « des cibles de choix »

Selon Ryan Olson de Palo Alto Networks Inc, « l'information n'est toutefois pas à prendre à la légère », puisque cela montre que l'AppStore peut être compromis par des hackers qui ciblent les développeurs. Pis, cela pourrait donner des idées à d'autres et il sera difficile de s'en prémunir, estime-t-il.

L'iPhone ne serait-il plus aussi sûr qu'à ses débuts ? « Avec l'augmentation des parts de marché d'Apple, le nombre de cibles augmente et l'intérêt des cybercriminels augmente », pointe Laurent Heslault, responsable des stratégies de sécurité chez Symantec. Gérome Billois, administrateur du Club de la sécurité de l'information français (Clusif), renchérit :

Surtout que les utilisateurs d'Apple sont connus pour avoir des revenus plus élevés, faisant d'eux des cibles de choix ».

Surtout que les utilisateurs d'iPhone – et plus largement de smartphones – n'ont pas encore pris pleinement conscience des risques de piratage sur ces mini-ordinateurs. Rien que l'an dernier, l'entreprise de sécurité Symantec a découvert 6,3 millions d'appli malicieuses capables d'infecter les terminaux.

Apple n'est donc pas beaucoup plus sûr que ses concurrents. Le rapport annuel de Symantec pointe que 84% des vulnérabilités découvertes le sont sur iPhone (contre 11% pour Android). Le plus souvent, elles sont exploitées pour infecter l'appareil, dérober des informations personnelles (mots de passe, comptes bancaires…), afficher des publicités, ou encore envoyer des SMS surtaxés. Laurent Heslault interroge :

Il y a des centaines de milliers d'applications gratuites disponibles, croyez-vous qu'il y ait autant de philanthropes ? »

La vigilance est donc de rigueur avant de cliquer sur un lien, entrer ses identifiants sur un site, etc. Même prudence lorsqu'une fenêtre pop-up s'ouvre sur l'iPhone, réclamant l'identifiant et le mot de passe iCloud. Si elle n'a pas de raison de s'ouvrir (par exemple lors de la consultation de ses e-mails), alors il n'y a pas de raison de lui donner les informations.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source : http://tempsreel.nouvelobs.com/tech/20150921.OBS6188/des-hackers-dupent-apple-et-infectent-des-millions-d-iphone.html
Par Boris Manenti

Un nouveau Virus vise les iPhones et l’iPads | Le Net Expert Informatique

	Un nouveau Virus vise les iPhones et l’iPads

Cette nouvelle #famille de virus, baptisée « #KeyRaider« , s'attaque à des iPhone et iPad débloqués pour y installer des applications non approuvées par Apple.

« Nous pensons que c'est le plus grand vol connu de comptes Apple causé par un virus », indique la société de sécurité informatique américaine Palo Alto Networks.©CAROLINE SEIDEL

Des chercheurs en sécurité informatique affirment avoir identifié une nouvelle famille de virus, baptisée « KeyRaider », qui s'attaque à des iPhone et iPad débloqués pour pouvoir y installer des applications non approuvées par Apple. « Nous pensons que c'est le plus grand vol connu de comptes Apple causé par un virus », indique la société de sécurité informatique américaine Palo Alto Networks sur son site internet, où elle résume les résultats d'une enquête réalisée avec WeipTech, un groupe technique amateur réunissant des fans d'Apple en Chine.

« KeyRaider a ainsi déjà réussi à voler plus de 225 000 comptes Apple valides » avec leurs mots de passe, qui ont été retrouvés stockés sur un serveur, ainsi que « des milliers de certificats, clés privées et tickets d'achats », précise Palo Alto Networks. Le virus fonctionne en interceptant les communications de l'appareil avec iTunes, la boutique de musique en ligne d'Apple. Il vole et partage des informations d'achats à l'intérieur d'applications et désactive la fonction de déblocage locale ou à distance de l'iPhone ou de l'iPad.

Dix-huit pays touchés

Certaines des victimes ont constaté des achats anormaux, d'autres ont vu leur appareil bloqué par des pirates qui leur ont demandé une rançon, indique encore la société de sécurité informatique. KeyRaider s'attaque aux appareils utilisant iOS, le système d'exploitation mobile d'Apple, qui ont été débloqués et est distribué en Chine par l'intermédiaire de Cydia, une application non officielle pour iOS donnant accès à des applications non validées par Apple.

Palo Alto Research estime au total que des consommateurs de 18 pays ont été touchés, dont la Chine mais aussi la France, la Russie, le Japon, le Royaume-Uni, les États-Unis, le Canada, l'Allemagne, l'Australie, Israël, l'Italie, l'Espagne, Singapour et la Corée du Sud.

Un porte-parole d'Apple a souligné dans un courriel que « le problème ne touche que ceux qui non seulement ont débloqué leurs appareils (pour permettre des utilisations non utilisées par le fabricant, NDLR) mais ont aussi téléchargé le virus depuis des sources non fiables ».

« L'iOS est conçu pour être fiable et sûr à partir du moment où on allume l'appareil. Pour protéger nos utilisateurs des virus, nous surveillons le contenu de l'App Store et nous assurons que toutes les applications dans l'App Store adhèrent aux lignes directrices fixées pour nos développeurs », a-t-il rappelé. Il a toutefois assuré qu'Apple avait pris « des mesures pour protéger ceux affectés par le problème en aidant les propriétaires à réinitialiser leurs comptes (en ligne) iCloud avec un nouveau mot de passe ».

Lire la suite….

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.lepoint.fr/high-tech-internet/piratage-informatique-l-iphone-et-l-ipad-vises-par-un-nouveau-virus-02-09-2015-1961181_47.php

---

Votre iPhone est débridé ? Alors vous l'avez rendu vulnérable | Le Net Expert

Informatique

Votre iPhone est débridé ? Alors vous l'avez rendu vulnérable

Quand la firme d'espionnage Hacking Team s'est faite détroussée de 400 gigaoctets de documents internes compromettants sur ses activités, ces derniers ont révélé des failles importantes dans les téléphones iPhone qui ont subi un débridage par leur propriétaire.

Débrider son iPhone le rendrait vulnérable aux intrusions.

La firme d'espionnage Hacking Team en Italie s'est fait prendre, le moins qu'on puisse dire, les «culottes baissées».

Imaginez une société privée, qui vend ses services aux plus offrants – généralement des gouvernements -, développe des procédés informatiques pour infiltrer et dérober à l'aide de logiciels espions et autres chevaux de Troie les ordinateurs de sociétés ou de gouvernements amis comme ennemis.

Et bien Hacking Team s'est fait littéralement détrousser de 400 Go de documents par un petit groupe de pirates qui les a mis en ligne. On y a appris beaucoup de choses, dont que les iPhone débridés par leur propriétaire les rendaient vulnérables aux intrusions.

Hacking Team dispose de moyens pour percer tout type de systèmes d'exploitation; Windows, Mac OS, Linux et les systèmes mobiles comme iOS, Android, Symbian et même BlackBerry.

Si l'espionnage de haute voltige ne concerne véritablement que les services de renseignements des gouvernements, il est intéressant de constater que les utilisateurs d'iPhone – c'est-à-dire vous et moi – deviennent potentiellement des cibles quand les appareils tournant sous iOS sont débridés (jailbreakés) par leurs utilisateurs.

À QUOI SERT DE DÉBRIDER SON IPHONE?

Le débridage permet de passer outre les verrouillages imposés par Apple pour ses téléphones iPhone. Ainsi, il devient possible d'installer des extensions non approuvées et accéder à toutes les fonctions du système.

À chaque mise à jour du système iOS (iOS 8.1, 8.2, 8.3), Apple colmate les brèches découvertes, mais les spécialistes du débridage trouvent toujours un moyen de contourner les parades.

En soi, débrider son appareil mobile n'est pas illégal, mais la manœuvre lui fait perdre sa garantie, auquel cas le propriétaire doit auparavant remettre en état son iPhone pour le faire réparer.

OUPS, DÉBRIDER OUVRE DES «PORTES» DU IPHONE

Dans le grand déballage de documents de Hacking Team, on apprend que les iPhone et iPad modifiés par débridage (tous deux roulent le même système iOS) devenaient vulnérables aux intrusions par ceux qui employaient les outils d'Hacking Team.

Pour environ 72 000 $, Hacking Team vendait au client un module de surveillance (snooping module) capable d'infiltrer les iPhone. Seul préalable, les appareils iOS devaient être débridés.

Note aux petits malins du bidouillage, votre iPhone «maison» a peut-être les portes grandes ouvertes, quel bel accueil pour les intrus!

Apple a depuis peu un argument de poids pour décourager la pratique du débridage. La société fait d'ailleurs tout en son possible pour empêcher les développeurs d'applications de sortir des limites permises d'iOS afin de protéger l'intégrité de son système mobile.

Plus encore, un iPhone débridé et infecté permet non seulement d'accéder à son contenu, mais de pénétrer les informations contenues dans l'ordinateur qui sert à sa synchronisation.

Avec tous les fichiers et applications «illégitimes» qui circulent librement sur les réseaux louches, l'idée de les croire tous «sains» et sans danger n'est que pur délire.

Pour terminer, les activités d'Hacking Team ciblent essentiellement les appareils de quelques individus en raison de leurs activités politiques, par exemple, les chances que vous soyez visé sont pratiquement nulles. Mais la leçon à retenir ici demeure que les protections qu'impose Apple à ses produits sont justifiées.

Quant à la pratique du débridage, elle vient de perdre des points.

Source : http://fr.canoe.ca/techno/materiel/mobiles/apple/archives/2015/08/20150806-120618.html

iPhone 6 à 1 euro – Une arnaque bien rodée | Le Net Expert Informatique

iPhone 6 à 1 euro – Une araque bien rodée

Diffusée partout, notamment sur les réseaux sociaux, cette arnaque qui débouche en fait sur des abonnements payants fait des dizaines de victimes, selon l'association de consommateurs.

Quand c'est trop beau, il faut se méfier… Allez dire ça aux victimes de Bernard Madhof qui promettait des placements assurant des rentabilité jamais vues ou à ceux qui ont cru à ces publicités proposant des iPhone 6 à 1 euro… Un iPhone à ce prix, personne ne devrait y croire, et pourtant…
Ils sont des dizaines à cliquer sur ces publicités qui pullulent actuellement sur la toile, notamment sur les sites de téléchargement ou via les réseaux sociaux. Au point que l'association de défense des consommateurs UFC Que Choisir s'en émeuve.
« Ces offres sentent le roussi à plein nez et pourtant, à en croire les messages qui arrivent sur différents forums Internet, leurs victimes se comptent par dizaines », souligne l'association qui a mené l'enquête.

Evidemment, en cliquant sur ces liens, point d'iPhone à l'horizon (ni de Galaxy S6 Edge, et encore moins d'Apple Watch) mais un abonnement surtaxé à un service quelconque.

Vrais-faux article de presse
« La page promotionnelle, au design et à la rhétorique soignés, invite l'internaute à saisir son adresse e-mail et à accepter les conditions générales. À l'étape suivante, il doit saisir ses coordonnées bancaires. Et, quelques jours plus tard, il constate qu'une somme rondelette, de 49 à 89 € selon les offres, a été débitée de son compte, en plus de l'euro prélevé initialement. Pire, ce prélèvement se répétera puisque l'internaute s'est en fait abonné à un site Internet de jeux en ligne, comme Rockyfroggy.com, un site de musique, comme Radioplanets.com, ou un club d'achat comme DealsOfToday.eu ou Wonkabonka.com », explique l'UFC.
Et ceux qui persistent à croire qu'ils recevront un jour leur précieux, peuvent attendre, longtemps. « En réalité, recevoir le produit promis n'est même pas garanti : il s'agit de lots que le nouvel inscrit peut potentiellement gagner, un gagnant étant le plus souvent « sélectionné » tous les 500 participants. L'euro payé par l'internaute lui ouvre en fait droit à une période d'essai de quelques jours aux services du site. Heureusement, d'après les témoignages lus sur les forums, ni la rétractation ni le désabonnement ne se semblent poser trop de problèmes ».
Le vrai problème, c'est la propagation massive et en augmentation de ces arnaques, sur Facebook, Twitter etc… « Il faut dire que Rockyfroggy, DealsOfToday et les autres usent de subterfuges variés et savent manifestement créer le « buzz ». Pour attirer les internautes à eux, ils arborent plusieurs « déguisements » dans lesquels ils glissent un lien vers leur page d'abonnement. Il peut s'agir d'une enquête de satisfaction émanant soi-disant de votre opérateur mobile, d'un jeu concours organisé par votre fournisseur d'accès à Internet, d'une note de blog imaginaire… »

Mieux, ces promos se glissent parfois dans des vraix-faux articles de presse. On a ainsi pu voir la charte graphique de La Tribune utilisée pour attirer le naïf… « Heureusement, les utilisateurs ne sont pas dupes », assure l'association, mais comme pour le spam, il suffit qu'un infime pourcentage clique pour faire le beurre de ces escrocs.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.zdnet.fr/actualites/iphone-6-a-1-euro-l-arnaque-fonctionne-plutot-bien-alerte-l-ufc-39819222.htm